Charles University
Faculty of Social Sciences
Department of Security Studies

Hybrid Warfare (JPM390)

Summer Semester 2024

6 ECTS

Wednesday 17:00 – 18:20, room C520 Jinonice

Register for this course also in Moodle

Course leader

Mgr. Michal Šenk (michal.senk@fsv.cuni.cz)

Office hours: Thursday 14:00 – 15:30; Wednesday 16:30 – 17:00 (upon prior request) (please register here)

External expert lecturer

Plk. Mgr. Otakar Foltýn

Former chief of Czech Military Police, officer of the Czech Army with experience with foreign mission deployment (Kosovo, Afghanistan), currently member of the Military Office of the President of the Czech Republic

Course description

The course aims to offer its prospective students the opportunity to broaden their knowledge about the phenomenon of *hybrid warfare* through a multifocal lens incorporating both theoretical (academic) and more practical, policy-oriented insights. The course departs from the assumption that hybrid warfare, increasingly a buzzword and very much a catch-all term, does not capture a radically new phenomenon in the history of humankind. Quite the opposite: if understood as an activity that "incorporates a range of different modes of warfare"[1], the case may well be made that warfare has *always* been hybrid. That said, it would be untenable to suggest that the kind of warfare we are experiencing nowadays does not have specific intrinsic qualities that set it apart from the warfare of the past. The modern battlefield is, indeed, in many ways more complex and even pernicious than the Flanders Fields (the amount of spilled blood is another matter). As such, (modern-day) hybrid warfare *is* worth our attention – provided we manage to turn it into a more viable analytical category. In this course, we aim to do just that: after showing that hybrid warfare is often little more than an empty label (and a *gross* oversimplification of history), we offer a better – and hopefully more useful – way of thinking about the phenomenon.

[1] Hoffman, F. G. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington, Virginia: Potomac Institute for Policy Studies.

We begin by situating the phenomenon within the broader context of warfare and strategy, complementing it with insights from (theories of) international security studies (ISS) and science and technology studies (STS) (session 3). Following that, we turn to unpack the specific properties of today's world that make the kind of warfare we call hybrid possible, focusing, inter alia, on the Janus-faced nature of the internet (social media) and the inherent vulnerability of open societies to warfare predicated on information (sessions 4 and 5). Having done that, we focus on two actors typically labeled as 'hybrid threats' – Russia and China – to illustrate how modern-day hybrid warfare operates in practice (sessions 6 and 7). It will be seen that, while the operational environment is the same, the tools and methods tend to differ substantively depending on the actor. The actor even *need not* be a state one, as we show subsequently (session 8). And, to ensure that our course is not unacademically Western-centric, we also show that hybrid warfare, far from the property of authoritarian states, may equally well be fought by democracies (session 9). Finally, we switch gears and turn to the hard part: if, as we seek to show, modern-day hybrid warfare is very much a *real* phenomenon (and a threat), what should we do about it? How should we counter it? Taking up these uneasy questions, in the last two substantive sessions (10 and 11), we focus on the ways, as well as the shortcomings thereof, of defending against hybrid threats.

Aims of the course

By way of this plan, this course aims both to dispel the often unhelpful understanding of hybrid warfare and turn it into a more productive analytical category, one at the same time grounded in a solid theoretical background and policy-relevant. Upon completing our course, the students should be able to:

- Critically discuss the definitional and conceptual properties of the phenomenon of hybrid warfare;
- Situate modern-day hybrid warfare in the (historical) context of warfare and strategy more generally;
- Pinpoint the intrinsic qualities of the current operational environment that defines the practice and possibilities of modern-day hybrid warfare;
- Describe various actors' approaches to hybrid warfare and explain their differences;
- Understand existing strategies of countering hybrid threats, assess their viability and suggest improvements.

Charles University
Faculty of Social Sciences
Department of Security Studies

Course requirements

ATTENDANCE:

To successfully complete the course, students can miss up to two sessions, provided the absences are excused beforehand and with a valid reason such as health issues, serious personal issues, study- or work-related reasons (work-related reasons will be excused only if the work has direct relevance for the student's career in the field of international security, like an internship at the Ministry of Defense or an IGO/NGO). If a student misses more than two sessions, or fails to notify the course leader in advance, their eligibility for the completion of the course will be decided on an individual basis and may be conditioned by additional course work.

ASSESSMENT:

The assessment for this course consists of four components. As explained in detail below, the minimum threshold for successfully passing the course is an aggregate 51 % scored across the components. However, students must score this percentage also in each component individually. In other words, it is not possible to skip a component and still pass the course. All four of the following must be successfully passed.

1. Weekly readings and discussion questions (20 %):

Each substantive session is assigned a selection of readings for the students to familiarize themselves with the topics to be discussed and to provide them with necessary background knowledge on the state of the art. This is critical: as the sessions are designed as a mixture of lecturing and discussing, students should already know the 'basics' and be prepared to critically examine them in turn. Thus, as a way of preparation, for each substantive session, students are required to read the **assigned literature** and answer **questions** related to them. The questions will appear in Moodle a week before the session takes place and students will have until the start of the session to write their answers. The number and scope of the questions will vary depending on the week's literature. However, each week, all questions must be answered.

2. Active participation in the sessions (10 %):

Students are not only required to read the literature but are also expected to actively **engage** in the sessions, be it by discussing, asking questions or taking part in group activities.

3. Group policy presentations (40 %):

The most important component of the course assessment requires the students to take part in the preparation and subsequent presentation of an original **policy analysis of an existing strategy of countering hybrid threats**. Depending on the size of the class, each student will be assigned to a group of 4-5 people that will collectively work to produce and successfully present an analysis of a real-world strategy that a state or another kind of international entity has designed and used for the purposes of countering hybrid threats. The presentations will be delivered during the two seminar sessions (10 and 11) – anticipating that there are four groups in total, two presentations per seminar. One presentation should take between 25 and 30 minutes and may be delivered by one group member, a selection of group members or the whole team. That being said, *all* group members are required to participate in the preparation of the presentation. Importantly, each group must prepare a short **two pager** containing the main points that will be presented and upload it in Moodle at least two days before the presentation.

> **SPECIFICATION**: The groups are expected to prepare their presentations in a highly analytical manner and respond to the issue areas of the following structure. To achieve the maximum amount of points to be awarded from this exercise, all outlined issue areas need to be addressed. When delivering their outputs, the groups are also advised to follow the structure.

- **Describe the main tenets of the strategy, its key parameters and objectives**:
  - What are its key characteristics?
  - Which goals does it seek to achieve?
  - Which threats does it identify and aim to counter?
- **Interpret the historical, political and strategic background of the strategy**:
  - In what historical context did the strategy originate?
  - Which internal and external factors drove and influenced its formulation?
  - How does it relate to the actor's overall security and defense strategy?
- **Explain how the strategy seeks to achieve its goals**:
  - What tools (military, legal, etc.) does the strategy envision to utilize?
  - Which actors (the army, secret services, the population, etc.) does it involve?
- **Assess the viability of the strategy and suggest improvements**:
  - Does the strategy identify viable objectives and relevant threats?
  - Does the strategy reflect the capacity of the actor to carry it out?
  - Do the allocated means and actors match the envisioned ends?
  - How could the strategy be improved?

3. Final exam (30 %):

Finally, to successfully pass the course, students will need to sit a final written exam (held in Moodle at three various occasions) that will test their knowledge of materials discussed during lectures and the assigned readings. The exam will comprise several open-ended questions, some shorter (testing the students grasp of the 'basics'), some longer (testing the students understanding of the subject matter and their ability to think about it critically).

Charles University
Faculty of Social Sciences
Department of Security Studies

Marking scale

General Grade	Grade Specification	Percentage
A – excellent	Excellent upper (1)	100 – 96
	Excellent lower (2)	95 - 91
B – very good	Very good upper (1)	90 – 86
	Very good lower (2)	85 – 81
C – good	Good upper (1)	80 – 76
	Good lower (2)	75 – 71
D – satisfactory	Satisfactory upper (1)	70 – 66
	Satisfactory lower (2)	65 – 61
E – sufficient	Sufficient upper (1)	60 – 56
	Sufficient lower (2)	55 – 51
F – fail		50 – 0

Course rules

The *Code of Study and Examination of Charles University in Prague* provides the general framework of study rules at the university. According to art. 6, par. 17 of this Code, "a student may not take any examination in any subject entered in his study plan more than three times, i.e. he shall have the right to two resit dates; no extraordinary resit date shall be permitted[…] If a student fails to appear for an examination on the date for which he has enrolled without duly excusing himself, he shall not be marked; the provision of neither this nor of the first sentence shall constitute the right to arrange for a special examination date."

Any written assignment composed by the student shall be an original piece. The practices of plagiarism, defined by the Dean's Provision no. 18/2015, are seen as "a major violation of the rules of academic ethics" and "will be penalized in accordance with Disciplinarian Regulations of the faculty."

This instructor believes academic honesty is the foundation of the entire enterprise of a university. The personal integrity policy works for both students and teachers. Students can expect that the instructor will treat them in a fair, honest, and impartial manner. The instructor also expects students to deal with him and with one another honestly.

Plagiarism* and cheating are violations of academic honesty because they steal from the original creator of the work. In addition, they violate the relationship of honesty between student and teacher as the student attempts to pass off work as his or her own which was produced by another. Further, plagiarism and cheating violate the bond of honesty among students themselves. Students who produce their assignments through long, hard work are being violated by those taking a shortcut through the misappropriation of another's work or knowledge. Most sadly, students who violate academic honesty cheat themselves of the chance to learn. Only in an environment of honesty can genuine learning occur and good citizenship be fostered.

Because academic honesty is treated as a serious matter, the course policy is one of zero tolerance for academic dishonesty. Cheating and plagiarism will not be tolerated. If you are caught cheating at any point during the course, you will automatically fail the course.

*PLAGIARISM – "the unauthorized use or close imitation of the language and thoughts of another author and the representation of them as one's own original work." Random House Unabridged Dictionary, 2nd ed. (New York: Random House, 1993).

Charles University
Faculty of Social Sciences
Department of Security Studies

Structure of the course

Session 1 (February 21, 2024): Introduction to the course

Session 2 (February 28, 2024): (Re)defining hybrid warfare (Šenk)

Readings:

1. Hoffman, F. G. (2007) Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, Virginia: Potomac Institute for Policy Studies, pp. 11-59.
2. Wither, J. K. (2016) ‘Making Sense of Hybrid Warfare.’ *Connections*, 15(2), pp. 73–87.
3. Libiseller, C. (2023) ‘”Hybrid warfare” as an academic fashion’, *Journal of Strategic Studies*, 46(4), pp. 858-880.
4. Mansoor, P. R. (2012) ‘Introduction: Hybrid Warfare in History’, in Murray, W. and Mansoor, P. R. (eds.) *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge University Press, pp. 1-17.
5. Sheenan, M. (2019) ‘The Evolution of Modern Warfare’, in Baylis, J., Wirtz, J. J. and Gracy, C. S. (eds.) *Strategy in the Contemporary World*. Oxford University Press, pp. 36-55.

Session 3 (March 6, 2024): Strategy, theory, and technology (Šenk)

Readings:

1. Clausewitz, C. v. (1832/1989) *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, New Jersey: Princeton University Press, ch. 1, pp. 75-89.
2. Aron, R. (1966) *Peace & War: A Theory of International Relations*. London and New York: Routledge, ch. 1: ‘Strategy and Diplomacy or On the Unity of Foreign Policy’, pp. 21-46, and ch. 3: ‘Power, Glory and Idea or On the Goals of Foreign Policy’, pp. 71-93.
3. Gray, C. S. (2016) ‘Chapter 2: Peace and war: politics at home and abroad’ in Strategy and Politics. Oxon: Routledge, pp. 23-35.
4. Orlikowski, W. J. (1992). ‘The Duality of Technology: Rethinking the Concept of Technology in Organizations.’ *Organization Science*, *3*(3), pp. 398–427.

Session 4 (March 13, 2024): The modern operational environment (Foltýn)

Readings:

1. Tzu, S. (1910/2009) *The Art of War*. Translated by Lionel Giles. Pax Librorium Publishing House, pp. 1-55.
2. Foltýn, O. (2018) ‘Playing football on a tennis court: What limitations do Western soldiers face when trying to understand the complex operational environment’, *Terrorism: An Electronic Journal and Knowledge Base* VII, 2, pp. 24-28.

3. BIS (2017) Annual Report of the Security Information Service for 2016, pp. 1-35.
4. Giegerich, B. (2016) 'Hybrid Warfare and the Changing Character of Conflict', *Connections*, 15(2), pp. 65-72.
5. Morris, J. (2019) 'Law, Politics, and the Use of Force', in in Baylis, J., Wirtz, J. J. and Gracy, C. S. (eds.) *Strategy in the Contemporary World*. Oxford University Press, pp. 108-126.

Session 5 (March 20, 2024): Democracy, open society, and information warfare
(Foltýn)

Readings:

1. Foltýn, O. (2022) 'What Is Happening to Democracies in the U.S. and in Europe?', *Journal of Policy & Strategy*, 2(3), pp. 137-140.
2. Harari, Y. N. (2019) *21 Lessons for the 21st Century*. London: Jonathan Cape, ch. 17.
3. RTO Task Group SAS-057, NATO (2006) *Information Operations – Analysis Support and Capabilities Requirements*, pp. 1-30.
4. Jaitner, M. and Mattsson, P. A. (2015) 'Russian Information Warfare of 2014', *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*. Tallinn: NATO CCD COE Publications, pp. 39-52.

Session 6 (March 27, 2024): Russia's approach to hybrid warfare (Foltýn)

Readings:

1. Bagge, D. P. (2019) *Unmasking Maskirovka: Russia's Cyber Influence Operations*. New York: Defense Press, pp. 27-70, 71-114.
2. Gressel, G. (2015) 'Russia's Quiet Military Revolution, and What it Means for Europe', *ECFR Policy Briefs*, 143, pp. 1-16.
3. Orenstein, H. (translator) (2019) 'Russian General Staff Chief Valery Gerasimov's 2018 Presentation to the General Staff Academy', *Military Review*, January-February, pp. 130-138.
4. Putin, V. (2006) 'Annual Address to the Federal Assembly. May 10, Marble Hall, the Kremlin, Moscow. Available at: en.kremlin.ru/events/president/transcripts/23577.
5. Galeotti, M. (2014) 'The "Gerasimov Doctrine" and Russian Non-Linear War', *In Moscow's Shadows*. Available here.

Session 7 (April 3, 2024): China's approach to hybrid warfare (TBA)

Readings:

1. Marks, T. A. and Ucko, D. H. (2021) 'Gray zone in red: China revisits the past', *Small Wars & Insurgencies*, 32(2), pp. 181-204.

2. Saalman, L. (2021) ‘China and its hybrid warfare spectrum’, in Weissmann, M. et al. (eds.) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris, pp. 95-112.
3. Harold, S. W. et al. (2021) *Chinese Disinformation Efforts on Social Media*. Santa Monica, Calif.: RAND, chapter 2: “Chinese Social Media–Based Disinformation Operations in Theory”, pp. 11-32, and chapter 3: “Chinese Social Media–Based Information Operations in Practice”, pp. 33-63.
4. Hung, T.-C. and Hung, T.-W. (2020) ‘How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars’, *Journal of Global Security Studies*, 7(4), pp. 1–18.
5. Patalano, A. (2018) ‘When strategy is “hybrid” and not “grey”: reviewing Chinese military and constabulary coercion at sea,’ *The Pacific Review*, 31(6), pp. 811-839.
6. Beeson, M. (2018) ‘Geoeconomics with Chinese characteristics: the BRI and China’s evolving grand strategy,’ *Economic and Political Studies*, 6(3), pp. 240-256.
7. Curtis, J. S. (2021) ‘Springing the “Tacitus Trap”: countering Chinese state-sponsored disinformation’, *Small Wars & Insurgencies*, 32:2, pp. 229-265.

Session 8 (April 10, 2024): Hybrid non-state actors (Šenk)

Readings:

1. Schroefl, J. and Kaufman, S. J. (2014) ‘Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War’, *Studies in Conflict & Terrorism*, 37(10), pp. 862-880.
2. Rauta, V. (2020) ‘Towards a typology of non-state actors in “hybrid warfare”: proxy, auxiliary, surrogate and affiliated forces’, *Cambridge Review of International Affairs*, 33(6), pp. 868-887.
3. Kiras, J. D. (2019) ‘Irregular Warfare: Terrorism and Insurgency’, in in Baylis, J., Wirtz, J. J. and Gracy, C. S. (eds.) *Strategy in the Contemporary World*. Oxford University Press, pp. 183-201
4. Phillips, V. (2017) ‘The Islamic State's Strategy: Bureaucratizing the Apocalypse through Strategic Communications’, *Studies in Conflict & Terrorism*, 40(9), pp. 731-757.
5. Azani, E. (2013) ‘The Hybrid Terrorist Organization: Hezbollah as a Case Study’, *Studies in Conflict & Terrorism*, 36(11), pp. 899-916.

Session 9 (April 17, 2024): Democracies as perpetrators of hybrid warfare (Šenk)

Readings:

1. Jervis, R. (2016) ‘Understanding the Bush Doctrine: Preventive Wars and Regime Change’, *Political Science Quarterly*, 131(2), pp. 285-311.
2. Börzel, T. A. and Lebanidze, B. (2017) ‘”The transformative power of Europe” beyond enlargement: the EU’s performance in promoting democracy in its neighbourhood’, *East European Politics*, 33(1), pp. 17-35.

3. Mearsheimer, J. J. (2018) The Great Delusion: liberal dreams and international realities. New Haven: Yale University Press, chapter 6: ‘Liberalism as a source of trouble’, pp. 152-187.
4. Chandler, D. (2006) *Empire in Denial: The Politics of State-building.* London: Pluto Press, chapter 1: “Introduction: Empire in Denial”, pp. 1-25, and chapter 5: “Denial of the EU’s Eastern Empire”, pp. 96-122.
5. Taylor, P. M. (2002) ‘Strategic Communications or Democratic Propaganda?’, *Journalism Studies*, 3(3), pp. 437-441.
6. Farwell, J. P. (2012) Persuasion and Power: The art of strategic Communication. Washington, D.C.: Georgetown University Press, “Introduction”, pp. xv-xxi, and “Chapter 1: Psychological Operations”, pp. 3-22.
7. Rashi, T. and Schleifer, R. (2023) ‘The Ethics of Psychological Warfare – Lessons from Israel’, *Democracy and Security*, 19(2), pp, 199-210.

Session 10 (April 24, 2024): Seminar – Defending against hybrid threats 1

Students’ presentations

Session 11 (May 15, 2024): Seminar – Defending against hybrid threats 2

Students’ presentations

Session 12 (May 22, 2024): Conclusions, final remarks, test preparation